

#4

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Katsutoshi NAKAMURA

Appln. No.: 10/027,233

Confirmation No.: 9112

Filed: December 27, 2001

For: APPARATUS AND METHOD FOR CONTROLLING LEVELS OF ACCESS  
PERMISSION



Group Art Unit: 2131

Examiner: NOT YET ASSIGNED

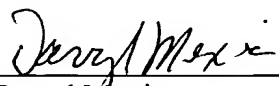
SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Submitted herewith is one (1) certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,

  
Darryl Mexic  
Registration No. 23,063

SUGHRUE MION, PLLC  
2100 Pennsylvania Avenue, N.W.  
Washington, D.C. 20037-3213  
Telephone: (202) 293-7060  
Facsimile: (202) 293-7860

Enclosures: Japan 2000-397129  
DM\mg\plr  
Date: March 14, 2002



印 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年12月27日

出 願 番 号

Application Number:

特願2000-397129

出 願 人

Applicant(s):

セイコーエプソン株式会社

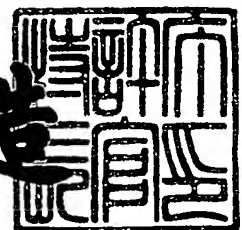


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年12月14日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3109370

【書類名】 特許願

【整理番号】 J00801272

【提出日】 平成12年12月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60  
H04L 12/24

【発明者】

【住所又は居所】 長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

【氏名】 中村 勝俊

【特許出願人】

【識別番号】 000002369

【氏名又は名称】 セイコーエプソン株式会社

【代理人】

【識別番号】 100099324

【弁理士】

【氏名又は名称】 鈴木 正剛

【手数料の表示】

【予納台帳番号】 031738

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0004318

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス権限レベル制御装置及び方法

【特許請求の範囲】

【請求項 1】 提供可能な情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の情報へのアクセスを許容するシステムにおいて実行される方法であって、

前記ユーザのアクセス要求の履歴に基づいて提供対象情報に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、

検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む、

アクセス権限レベルの制御方法。

【請求項 2】 使用可能な一又は複数の装置の範囲を定める複数レベルのアクセス権限のいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の前記一又は複数の装置の使用を許容するシステムにおいて実行される方法であって、

前記ユーザのアクセス要求の履歴に基づいて使用対象である一又は複数の装置に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、

検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む、

アクセス権限レベルの制御方法。

【請求項 3】 要求に応じてユーザの操作する端末に処理機能を付加するためのデジタル情報の提供を行うコンピュータシステムであって、提供可能なデジタル情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザに割り当てられており、アクセス権限を伴うユーザか

らのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲のデジタル情報の提供を許容するシステムにおいて実行される方法であって、

前記ユーザのアクセス要求の履歴に基づいて提供対象のデジタル情報に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、

検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む、

アクセス権限レベルの制御方法。

【請求項 4】 ユーザを識別するためにユーザ自身により設定可能な識別情報をユーザ毎に保持するステップと、

前記アクセス要求の際に要求元であるユーザに識別情報の入力を促し、入力された識別情報を用いたユーザの識別が正常に行われることを前記許容の条件として定めるステップとをさらに含み、

前記検出するステップは、最も最近行われた識別情報設定後の履歴に基づいて前記関心度合い及び／又はその変化を検出する、

請求項 1 ないし 3 のいずれか記載のアクセス権限レベルの制御方法。

【請求項 5】 前記検出された関心度合い及び／又はその変化が、所定の条件を満足するときに、前記アクセス要求元のユーザに対して識別情報の更新を促すステップをさらに含む、

請求項 4 記載のアクセス権限レベルの制御方法。

【請求項 6】 前記検出された関心度合い及び／又はその変化が、アクセス要求回数が所定回数を越えたことを示す場合、前記アクセス要求元のユーザに対して識別情報の更新を促すステップをさらに含む、

請求項 4 記載のアクセス権限レベルの制御方法。

【請求項 7】 前記識別情報の更新が行われなかったときに、前記アクセス要求元のユーザに割り当てられている現在のアクセス権限のレベルを、このレベルにより定められる範囲より狭いレベルに変更するステップをさらに含む、

請求項 5 又は 6 記載のアクセス権限レベルの制御方法。

【請求項 8】 ユーザ自身に関する情報の提供と引き替えにこのユーザを識別するための識別情報と、提供された情報内容に応じたレベルのアクセス権限とを割り当てるステップと、

前記アクセス要求の際に、割り当てられた識別情報の入力を要求元であるユーザに促し、入力された識別情報を用いたユーザの識別が正常に行われることを前記提供の条件として定めるステップとをさらに含み、

前記検出するステップは、最も最近行われたアクセス要求時からの履歴に基づいて前記関心度合い及び／又はその変化を検出する、

請求項 1 ないし 3 のいずれか記載のアクセス権限レベルの制御方法。

【請求項 9】 前記検出された関心度合い及び／又はその変化が、所定の条件を満足するときに、前記アクセス要求元のユーザに対してユーザ自身に関する情報の提出を再度促すステップをさらに含む、

請求項 8 記載のアクセス権限レベルの制御方法。

【請求項 1 0】 前記検出された関心度合い及び／又はその変化が、前記最も最近行われたアクセス要求時から所定日数が経過したことを示す場合、前記アクセス要求元のユーザに対してユーザ自身に関する情報の提供を再度促すステップをさらに含む、

請求項 8 記載のアクセス権限レベルの制御方法。

【請求項 1 1】 前記情報を再度促すステップに応じて、ユーザ自身に関する情報の提供が行われなかったときに、前記アクセス要求元のユーザに割り当てられている現在のアクセス権限のレベルを、このレベルにより定められる範囲より狭いレベルに変更するステップをさらに含む、

請求項 9 又は 1 0 記載のアクセス権限レベルの制御方法。

【請求項 1 2】 前記情報を再度促すステップに応じて、前記ユーザ自身に関する情報の提供が行われなかったときに、このユーザに割り当てられた識別情報を抹消するステップをさらに含む、

請求項 9 又は 1 0 記載のアクセス権限レベルの制御方法。

【請求項 1 3】 提供可能な情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、ア

クセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の情報へのアクセスを許容するコンピュータシステムに適用される装置であって、

前記ユーザのアクセス要求の履歴に基づいて提供対象情報に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、

前記関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能とする手段とを備えるアクセス権限レベルの制御装置。

【請求項 1 4】 使用可能な一又は複数の装置の範囲を定める複数レベルのアクセス権限のいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の前記一又は複数の装置の使用を許容するコンピュータシステムに適用される装置であって、

前記ユーザのアクセス要求の履歴に基づいて使用対象である一又は複数の装置に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、

前記関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能とする手段とを備えるアクセス権限レベルの制御装置。

【請求項 1 5】 要求に応じてユーザの操作する端末に処理機能を付加するためのデジタル情報の提供を行うコンピュータシステムであって、提供可能なデジタル情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザに割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲のデジタル情報の提供を許容するシステムに適用される装置であって、

前記ユーザのアクセス要求の履歴に基づいて提供対象のデジタル情報に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、

検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にする手段と

を備えるアクセス権限レベルの制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ユーザに対して情報提供などのサービスを行うためのシステムに適用可能な装置及び方法に関し、特に、提供対象となる情報などの範囲を定めるためのアクセス権限のレベルに従ってサービスを行うシステムに適用可能な装置及び方法に関する。

【0002】

【従来の技術】

従来より、製品の販売促進や宣伝を目的として、対象となる製品及びそれに関連した情報を通信網を介して不特定多数のユーザに提供するサービスが行われている。近年では、情報提供を行う者（以降、「運営者」と称する）がホームページを開設し、会員化されたユーザにIDを発行し、一定の制限枠のなかで会員へのサービスを提供している。会員には非会員に比べ、より高いアクセス権を与えることで、運営者は会員と非会員との間で情報提供サービスの差別化を行うことができる。

【0003】

さらに運営者は、提供可能な情報の範囲を定める複数レベルのアクセス権限を会員毎に予め割り当てておき、このアクセス権限に従った情報の提供を行うことが多い。例えば、ホームページ上に段階的に掲示された情報のうち、どこまでの段階をアクセスしてきた会員に提供するかをアクセス権限のレベルに従って制御する。

【0004】

【発明が解決しようとする課題】

運営者側では、ユーザを会員とする場合、ユーザの個人情報の提供を前提で行うことが多い。しかし、ユーザは一般的に自己の個人情報の提供を行うことに対しては慎重であり、個人情報の過度の提供要求は会員募集の妨げとなる場合がある。このため、運営者側はより多くの個人情報の提供を受けることできめの細か



いサービスの提供につながることを承知の上で、提供される個人情報量と提供するサービスの質との間で適当な妥協点を設定しなくてはならない。

## 【 0 0 0 5 】

また、会員となったユーザであってもアクセス頻度が高い優良会員と、アクセス頻度が低い又はアクセスのほとんど無い会員とが存在する。このため、両者への情報の差別化の必要性があるにもかかわらず、同一のサービス提供を行わなくてはならない。さらに、長期会員もしくはアクセス頻度の高い会員には一般的にポイント制と称される履歴加算制度を用いて優遇処置を講じる場合があるが、前述した従来のサービス形態では実現することができない。

## 【 0 0 0 6 】

この他、近年では会員からの要求に応じ、自身の有する周辺機器へのアクセスや使用を許可したり、プログラムを提供することにより会員の使用する端末に特定の機能を付加させるなどのサービスも行われている。このような形態においても、先に述べた情報提供の場合と同様の問題がある。

また、不特定多数のユーザを相手とするサービスでは、情報の機密性、いわゆるセキュリティの維持も必要とされている。

## 【 0 0 0 7 】

このような実情により、本発明は、各ユーザに対して妥当な範囲内でサービスを行うための技術の提供を課題とする。そして、提供対象物の範囲を定める複数レベルのアクセス権限をユーザ毎に適宜制御するための装置及び方法を提供することを目的とする。

## 【 0 0 0 8 】

## 【課題を解決するための手段】

本発明によれば、提供対象物の範囲を定める複数レベルのアクセス権限をユーザ毎に適宜制御するための方法及び装置が提供される。

## 【 0 0 0 9 】

本発明による第1のアクセス権限レベルの制御方法は、提供可能な情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求

があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の情報へのアクセスを許容するシステムにおいて実行される方法であって、前記ユーザのアクセス要求の履歴に基づいて提供対象情報に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む。この第1の制御方法によれば、ユーザに対して妥当な範囲内の情報提供を行うためのアクセス権限レベルの制御を実現することができる。ここで提供される情報には、情報提供者が販売促進や宣伝の対象とする製品に関する情報などが該当する。

## 【 0 0 1 0 】

本発明による第2のアクセス権限レベルの制御方法は、使用可能な一又は複数の装置の範囲を定める複数レベルのアクセス権限のいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の前記一又は複数の装置の使用を許容するシステムにおいて実行される方法であって、前記ユーザのアクセス要求の履歴に基づいて使用対象である一又は複数の装置に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む。この第2の制御方法によれば、ユーザに対して妥当な範囲内で一又は複数の装置の使用を許容するためのアクセス権限レベルの制御を実現することができる。一又は複数の装置には、プリンタや大容量の記憶装置などが含まれる。

## 【 0 0 1 1 】

本発明による第3のアクセス権限レベルの制御方法は、要求に応じてユーザの操作する端末に処理機能を付加するためのデジタル情報の提供を行うコンピュータシステムであって、提供可能なデジタル情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザに割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲のデジタル情報の提供を許

容するシステムにおいて実行される方法であって、前記ユーザのアクセス要求の履歴に基づいて提供対象のデジタル情報に対する前記ユーザの関心度合い及び／又はその変化を検出するステップと、検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にするステップとを含む。この第3の制御方法によれば、ユーザに対して妥当な範囲内のデジタル情報提供を行うためのアクセス権限レベルの制御を実現することができる。このデジタル情報には、提供先の端末やコンピュータで実行可能なプログラムが含まれる。

## 【 0 0 1 2 】

このような第1～第3のアクセス権限レベルの制御方法は、ユーザを識別するためにユーザ自身により設定可能な識別情報をユーザ毎に保持するステップと、前記アクセス要求の際に要求元であるユーザに識別情報の入力を促し、入力された識別情報を用いたユーザの識別が正常に行われることを前記許容の条件として定めるステップとをさらに含み、前記検出するステップは、最も最近行われた識別情報設定後の履歴に基づいて前記関心度合い及び／又はその変化を検出してもよい。

## 【 0 0 1 3 】

このようなアクセス権限レベルの制御方法の場合、前記検出された関心度合い及び／又はその変化が、所定の条件を満足するときに、前記アクセス要求元のユーザに対して識別情報の更新を促すステップをさらに含んだり、前記検出された関心度合い及び／又はその変化が、アクセス要求回数が所定回数を越えたことを示す場合、前記アクセス要求元のユーザに対して識別情報の更新を促すステップをさらに含んでもよい。

さらに、識別情報の更新が行われなかったときに、前記アクセス要求元のユーザに割り当てられている現在のアクセス権限のレベルを、このレベルにより定められる範囲より狭いレベルに変更するステップをさらに含んでもよい。

## 【 0 0 1 4 】

また、第1～第3のアクセス権限レベルの制御方法は、ユーザ自身に関する情報の提供と引き替えにこのユーザを識別するための識別情報と、提供された情報

内容に応じたレベルのアクセス権限とを割り当てるステップと、前記アクセス要求の際に、割り当てられた識別情報の入力を要求元であるユーザに促し、入力された識別情報を用いたユーザの識別が正常に行われることを前記提供の条件として定めるステップとをさらに含み、前記検出するステップは、最も最近行われたアクセス要求時からの履歴に基づいて前記関心度合い及び／又はその変化を検出してもよい。

## 【 0 0 1 5 】

このようなアクセス権限レベルの制御方法の場合、前記検出された関心度合い及び／又はその変化が、所定の条件を満足するときに、前記アクセス要求元のユーザに対してユーザ自身に関する情報の提出を再度促すステップをさらに含んだり、前記検出された関心度合い及び／又はその変化が、前記最も最近行われたアクセス要求時から所定日数が経過したことを示す場合、前記アクセス要求元のユーザに対してユーザ自身に関する情報の提供を再度促すステップをさらに含んでもよい。

さらに、前記情報を再度促すステップに応じて、ユーザ自身に関する情報の提供が行われなかったときに、前記アクセス要求元のユーザに割り当てられている現在のアクセス権限のレベルを、このレベルにより定められる範囲より狭いレベルに変更するステップをさらに含んだり、このユーザに割り当てられた識別情報を抹消するステップをさらに含んでもよい。

## 【 0 0 1 6 】

本発明による第 1 のアクセス権限レベルの制御装置は、提供可能な情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の情報へのアクセスを許容するコンピュータシステムに適用される装置であって、前記ユーザのアクセス要求の履歴に基づいて提供対象情報に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、前記関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能とする手段とを備える。

## 【0017】

本発明による第2のアクセス権限レベルの制御装置は、使用可能な一又は複数の装置の範囲を定める複数レベルのアクセス権限のいずれかのレベルのアクセス権限がユーザ毎に割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲の前記一又は複数の装置の使用を許容するコンピュータシステムに適用される装置であって、前記ユーザのアクセス要求の履歴に基づいて使用対象である一又は複数の装置に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、前記関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能とする手段とを備える。

## 【0018】

本発明による第3のアクセス権限レベルの制御装置は、要求に応じてユーザの操作する端末に処理機能を付加するためのデジタル情報の提供を行うコンピュータシステムであって、提供可能なデジタル情報の範囲を定める複数レベルのアクセス権限のうちのいずれかのレベルのアクセス権限がユーザに割り当てられており、アクセス権限を伴うユーザからのアクセス要求があったときにこのユーザによる前記アクセス権限のレベルに適合する範囲のデジタル情報の提供を許容するシステムに適用される装置であって、前記ユーザのアクセス要求の履歴に基づいて提供対象のデジタル情報に対する前記ユーザの関心度合い及び／又はその変化を監視する手段と、検出された関心度合い及び／又はその変化に応じて前記ユーザに割り当てられている現在のアクセス権限のレベルを他のレベルに変更可能にする手段とを備える。

前述した方法及び装置においては、対象物の提供によるサービスを運営する運営者にとって前述したユーザには、サービス提供の差別化を図る会員と非会員との両者が含まれる。

## 【0019】

## 【発明の実施の形態】

## &lt;第1実施形態&gt;

以下、図面を参照して本発明を適用した処理環境提供システムについて説明する。

図 1 は、本発明を適用した処理環境提供システム 1 がネットワーク 3 を介してユーザの操作する端末 2-1~2-n (n は実数、以降、サフィックスは省略する) に処理環境を提供する形態を示している。端末に提供される処理環境とは、処理環境提供システム 1 に備えられている 1 つ又は複数の装置の使用と、ソフトウェア (デジタル情報) をダウンロードして実行することによる処理機能の付加とがある。1 つ又は複数の装置には、大容量の記憶装置や大判用のプリンタなどが含まれる。すなわち、この処理環境提供システム 1 は、アクセスされた端末 2 に対してソフトウェア又はハードウェアによる処理環境を構築するための提供を行う。

#### 【0020】

処理環境提供システム 1 は、通信制御部 11、環境提供制御部 12、装置群 13a、プログラム記憶部 13b、アクセス権限レベル制御部 14、ID テーブル管理部 15、及び、ID データベース 16 を含んだ構成となっている。

通信制御部 11 は、ネットワーク 3 を介した端末 2 との間の情報の送受信を制御する。通信制御部 11 は、受信した情報を適宜アクセス権限レベル制御部 14 に送ったり、端末 2 と環境提供制御部 12 との間の通信を制御する。環境提供制御部 12 は、端末 2 と装置群 13a 及びプログラム記憶部 13b との間での接続及び配信の制御を行う。この際、環境提供制御部 12 は、アクセス権限レベル制御部 14 からユーザ毎に定められたアクセス権限レベルを予め受け取り、このアクセス権限レベルに従った接続及び配信を許可する。

#### 【0021】

装置群 13a は、大容量の記憶装置や大判のプリンタなどの各種ハードウェア装置により構成される。プログラム記憶部 13b は、端末 2 に処理機能を付加するためのソフトウェアが記憶されている。このようなソフトウェアは、特定の言語処理を可能とするためのプログラムや、特定の開発ツールなどを含む。

#### 【0022】

アクセス権限レベル制御部 14 は、ユーザ毎 (会員、非会員を含む) に提供可

能な処理環境の範囲を示すアクセス権限レベルを、その提供対象環境に対するユーザの関心度合い及び／又はその変化に従って制御する。この第1実施形態における、アクセス権限レベルとは「シェル」が該当する。「シェル」とは、UNIXにおいてログイン時にユーザがどのような使用環境で端末2上で処理を行えるかを定めたプログラム（モジュール）の一種である。また、この第1実施形態における関心度合い及び／又はその変化を検出するための情報として、アクセス数に対応するパスワードの変更回数を用いている。

## 【 0 0 2 3 】

IDテーブル管理部15は、IDデータベース16に保持されているIDテーブルの読み出しや書き込みを行う。IDデータベース16は、ユーザ毎にパスワード、アクセスカウント数、シェルなどの情報が記憶されているIDテーブルを保持している。端末2は、通信機能を有する汎用コンピュータを適用することができる。ネットワーク3には、LAN(local area network)などの通信網が適用される。

## 【 0 0 2 4 】

次に、前記IDデータベース16に保持されているIDテーブルの一例を図2を参照して説明する。

「ID」は、それぞれ管理者を含むユーザや、最も処理環境の狭いシェルが割り当てられているゲストを示す情報である。「パスワード」は、対応するIDを認識するために用いられ、ユーザなどが自発的に設定・変更できる。「アクセスカウント」は、ID毎に、パスワードが設定・変更されてからの処理環境提供システム1へのログイン回数を示し、パスワードが変更されるたびにリセットされる。

## 【 0 0 2 5 】

「プライオリティカウント」は、パスワードの変更要求の判定に用いられる情報である。この第1実施形態では、パスワードの変更頻度を高くすることが要求されるシステム管理者については30回、一般のユーザについては10.0回を判定回数となるように設定されている。これは、一般に、システム管理者が使用できる処理環境はユーザのそれに比べて広いためであり、このような設定はセキュ

リティの向上につながる。なお、プライオリティカウントはシステム管理者のみが変更可能となっている。

## 【 0 0 2 6 】

「ログインシェル」は、ユーザがログインした直後に実行されるシェルを格納しているディレクトリの位置を表す。なお、この第1実施形態においては、パスワードの変更が所定の条件を満足していない場合、ゲストとしてログインしたユーザと同じシェルが設定される。これによって、後述するユーザ独自の処理環境が制限される。

## 【 0 0 2 7 】

「オリジナルシェル」は、各ユーザに対して設定されており、対応するユーザに対して本来実行されるべきシェルを格納しているディレクトリの位置を表す。この第1実施形態では、オリジナルシェルはユーザの登録時にシステム管理者により設定できるような構成となっている。

## 【 0 0 2 8 】

次に、この第1実施形態において、ユーザからログインを受け付けてからそのユーザに対応するシェルを実行するまでの動作を図3～図7を参照して説明する。

まず、アクセス権限レベル制御部14は、通信制御部11を介してユーザからのアクセスを受け付けると図4に示されるようなログイン画面がユーザの操作する端末2上で表示されるように必要な情報を端末2宛に送出する。端末2において、表示された画面に従ってIDとパスワードとが入力されると、この情報が処理環境提供システム1に送出される。アクセス権限レベル制御部14はこの情報を受け取ると、IDとパスワードとの照合処理を行い、予め登録されているユーザであるか否かを判断する。登録されたユーザであることの照合が完了するとIDテーブルに登録されているアクセスカウントとプライオリティカウントとが読み出され、それぞれ、変数Ac、Pcに代入される（ステップS101）。この後、アクセス権限レベル制御部14は、各変数を比較し、AcがPcを越えているか否かを判定する（ステップS102）。

## 【 0 0 2 9 】



A c が P c を越えている場合（ステップ S 1 0 2 : YES）、アクセスを受け付けたユーザに対応するログインシェルが「/user/guest」となるように I D テーブルが書き換えられる。この後、アクセス権限レベル制御部 1 4 は、ユーザの操作する端末 2 に図 5 に示される画面が表示されるように情報を送出する。これにより、ユーザに対してパスワードの変更が要求されることになる（ステップ S 1 0 4）。

この画面に沿ってユーザからパスワードの変更が行われた場合（ステップ S 1 0 5 : YES）、ログインシェルがオリジナルシェルと同じになるように I D テーブルが書き換えられ、さらに、A c に 0 が代入される（ステップ S 1 0 6）。この後、A c の値が I D テーブルに反映されるように、I D テーブルが書き換えられ、アクセスしたユーザのログインシェルが実行される（ステップ S 1 0 7）。

#### 【0030】

A c が P c を越えていない場合（ステップ S 1 0 2 : NO）、すなわち、アクセスカウントがプライオリティカウントを越えていない場合には A c が 1 だけインクリメントされる（ステップ S 1 0 8）。また、ステップ S 1 0 4 において要求されたパスワードの変更に応じなかった場合（ステップ S 1 0 5 : NO）の場合も同様な処理が行われる。いずれの場合も、変更された A c の値が I D テーブルに反映されるように、I D テーブルが書き換えられ、アクセスしたユーザのログインシェルが実行される（ステップ S 1 0 7）。

パスワードの変更要求に従わなかった場合の I D テーブル例を図 7 に示す。ここでは、I D がユーザ 2 であるユーザは、パスワードが従来そのままログインシェルが「/user/guest」に書き換えられている。

#### 【0031】

以上の処理において、アクセス権限レベル制御部 1 4 によるアクセス権限レベル（シェル）の制御が行われる。特に、パスワードの変更が要求されたにもかかわらず、パスワードの変更を行わなかったユーザには、ゲストと同様のシェルが割り当てられる。このため、本来自己に割り当てられているシェルよりも処理環境が制限されたシェルが割り当てられることになる。このため、ユーザは、セキュリティに対する意識を高く持ち、アクセス数に対して所定頻度以上のパスワード

ドの書き換えを実行することが促される。

【 0 0 3 2 】

例えば、図 2 の I D テーブルに登録されている I D 「ユーザ 2」のユーザがシステム 1 にアクセスした場合、アクセスカウントがプライオリティカウントを越えているため、パスワードの更新が要求される。この要求に応じてユーザがパスワードの変更を行うと、図 6 に示されるように新たなパスワードが登録されると共に、アクセスカウントが 0 に戻される。

もし、ユーザがパスワードの変更を拒否した場合、アクセスカウントが 1 だけインクリメントされると共に、ログインシェルがゲストのものと同様に書き換えられ、本来自己に割り当てられている処理環境よりも制限された環境での処理が余儀なくされる。

【 0 0 3 3 】

なお、ログインシェルが一旦ゲストと同様の者に変更されたユーザであっても、システム 1 にアクセスする度にパスワードの変更が要求されるため、これに応じることにより本来のシェルに従った処理環境を取り戻すことができる。

また、ステップ S 1 0 7 以降では、ログインシェルがアクセス権限レベル制御部 1 4 から環境提供制御部 1 2 に通知され、この環境提供制御部 1 2 がログインシェルを実行する。これにより、ユーザは、アクセス権限レベル制御部 1 4 により制御されたアクセス権限レベルに従った装置群 1 3 a の使用許可、プログラム記憶部 1 3 b に記憶されているソフトウェアの配信が可能となる。

【 0 0 3 4 】

パスワードの変更は、アクセスカウントがプライオリティカウントを越えたときのみに可能なものではなく、ユーザの希望に応じて随時可能となり、その度に I D テーブルのアクセスカウントが 0 に戻される。

この第 1 実施形態では、関心度合及び／又はその変化を検出するための情報としてアクセス数に対応するパスワードの変更回数をもちいているがこれに限らない。例えば、最終アクセス日やパスワード変更日（設定日）からの経過時間（経過日数）に基づいて関心度合い及び／又はその変化を検出するようにしてもよい。さらに、I D テーブルを多重化し、これらの情報全体から関心度合い及び／又

はその変化を検出するように構成することもできる。

また、シェルは、処理環境に多様な範囲が設定可能である場合、これに従って多種のシェルを設定することができる。

【 0 0 3 5 】

#### <第 2 実施形態>

以下、図面を参照して本発明を適用した情報提供システムについて説明する。

図 8 は、本発明を適用した情報提供システム 4 が回線網を介して不特定多数のユーザに情報を提供（配信）するための一形態を示している。同図において、情報提供システム 4 は、不特定多数のユーザが操作する端末 2 - 1 ~ 2 - n（n は実数、以降、サフィックスは省略する）にネットワーク 3 を介して接続されている。これにより情報提供システム 4 と端末 2 との間で双方向通信が可能となる。なお、端末 2 及びネットワーク 3 は前述した第 1 の実施形態と同様であるので同じ参照符号を付している。

【 0 0 3 6 】

情報提供システム 4 は、通信制御部 4 1、情報提供制御部 4 2、コンテンツデータベース 4 3、アクセス権限レベル制御部 4 4、ID テーブル管理部 4 5、及び、ID データベース 4 6 を含んでいる。

通信制御部 4 1 は、ネットワーク 3 を介した端末 2 との間の情報の送受信を制御する。通信制御部 4 1 は、受信した情報を適宜アクセス権限レベル制御部 4 4 に送り、情報提供制御部 4 2 から送られるコンテンツデータを所望の端末 2 宛に送出する。情報提供制御部 4 2 は、コンテンツデータベース 4 3 からコンテンツデータを読み出し、これを通信制御部 4 1 に送る。この際、情報提供制御部 4 2 は、アクセス権限レベル制御部 4 4 からユーザ毎に定められたアクセス権限レベルを予め受け取り、このアクセス権限レベルに従った範囲内のコンテンツデータのみを通信制御部 4 1 に送る。

【 0 0 3 7 】

コンテンツデータベース 4 3 は、情報提供システム 4 を運営・管理する者が所望の製品の販売促進や宣伝という目的を達成するための情報をデジタル化されたコンテンツデータとして保持する。また、コンテンツデータは、例えば、インタ

ーネットのホームページに掲載するための情報である場合、端末 2 の画面に情報の種類や内容に応じて段階的に表示されるような形式でコンテンツデータベース 4 3 に保持されている。具体的には、情報の所在を示す URL (uniform resource locators) を、情報の種類や内容毎に使い分けて保持する。以下、コンテンツデータがホームページ用のデジタルデータであるとして説明する。

## 【 0 0 3 8 】

アクセス権限レベル制御部 4 4 は、ユーザ毎に提供可能な情報の範囲を示すアクセス権限レベルを、コンテンツデータとして保持されている製品やそれに関する情報へのユーザの関心度合い及び／又はその変化に従って制御する。この第 2 実施形態における、アクセス権限レベルとは後述する「プライオリティレベル」を示す。また、関心度合及び／又はその変化を検出するために、最終アクセス日からの経過日数が用いられる。

## 【 0 0 3 9 】

ID テーブル管理部 4 5 は、ID データベース 4 6 に保持されている ID テーブルの読み出しや書き込みを行う。ID データベース 4 6 は、ユーザ毎にパスワード、最終アクセス日、プライオリティレベルなどの情報が記憶されている ID テーブルを保持している。

端末 2 は、通信機能を有する汎用コンピュータを適用することができる。ネットワーク 3 には、端末 2 と情報提供システム 4 とを接続する公衆回線網を適用することができる。

## 【 0 0 4 0 】

次に、ID データベース 4 6 に保持されている ID テーブル例を図 9 を参照して説明する。

「ID」は、管理者や、各ユーザや、初めてこのホームページにアクセスするゲスト（非会員）を示す情報である。「パスワード」は、対応する ID を認識するために用いられ、ユーザ（会員）などが自発的に設定・変更できる。「最終アクセス日」は、対応するユーザがシステム 4 にアクセスした最も最近の年月日を示す。最初の 1 回しかアクセスしていないユーザは、この最初のアクセス日、すなわち登録した年月日となる。

## 【 0 0 4 1 】

「プライオリティレベル」は、ユーザ毎に割り当てられるアクセス権限レベルであり、このレベルに従って提供可能な情報の範囲が定められている。この第2実施形態では、「0」～「4」までの5段階のレベルのいずれかが割り当てられる。なお、最も広い情報範囲が提供可能となるレベルが0であり、以降数字の昇順に伴って提供可能となる情報の範囲が制限される。

## 【 0 0 4 2 】

「スタートページ」は、ログインしたユーザが最初に閲覧できるWebページを示すHTML(hypertext markup language)である。この第2実施形態では、各Webは一般的な名付けがなされている。「tour.html」はホームページのサイトマップ(構造)や内容のオーバビューを見せることができるものであり、ゲストユーザの初期Webページとして提供されている。「index.html」は各レベル毎の初期Webページを意味する。「admin.html」は管理者用Webページを意味する。

なお、図9のIDテーブルにおいて、IDが「ユーザ302」のエントリは、現在空きであり、パスワード、最終アクセス日、プライオリティレベル、スタートページの項に対応する欄にはデフォルトデータが登録されている。

## 【 0 0 4 3 】

次に、情報提供システム4へのID登録処理について説明する。情報提供システム4は、情報提供を要求するユーザからのアクセスに応じ所定の画面を端末2に表示させるための処理を行う。

## 【 0 0 4 4 】

ここで端末2に表示される画面例を図10に示す。この画面は大きく5つの領域に分類することができる。1番上の領域は、既にIDを取得したユーザ向けの領域である。2番目の領域はIDの取得を希望しないユーザ向けの領域であり、この領域からホームページに入った場合、ユーザはゲストとした扱われ最も狭い情報提供の範囲内でのみ情報提供が可能となる。3番目の領域は、IDの取得は要求するが、ユーザが自己の情報提供を望まない場合での登録領域である。

残りの2つの領域の内、一つはユーザが自己の名前と電話番号を提供すること

でIDを取得するための領域であり、もう一つはユーザが自己の名前、電話番号、住所、性別、年齢を提供することによってIDを取得するための領域である。

【0045】

ここで、ユーザがID「ユーザ302」を取得した場合に更新されるIDテーブル例を図11及び図12に示す。図11は、図10に示されるIDのみの取得でユーザが情報提供を要求した場合のテーブル例である。ここでは、IDのみの取得であるため、ID「ユーザ302」が付与されるだけで、パスワードの設定は不要となり、対応するプライオリティレベルが3、スタートページが/level1/level2/level3/index.htmlとなる。

【0046】

図12は、ユーザが名前と電話番号を提供することによりIDを取得した場合のIDテーブルの例である。ここでは、ユーザの希望によるパスワードが設定されると共に、プライオリティレベルが2、スタートページが/level1/level2/index.htmlとなる。ただし、いずれの登録であっても、その登録が行われた日付が最終アクセス日としてIDテーブルに登録される。

また、ユーザから通知された名前や電話番号などの情報は、図示せぬ記憶部に記憶される。ここで記憶された情報は、情報提供システム4を運営・管理する者が、個人のプライバシーを侵害しない範囲で利用可能なように記憶する構成でもよい。

【0047】

次に、図13～図15を参照して、既にIDを取得したユーザ、又はIDの取得を望まないユーザのアクセスに応じた情報提供システム4の動作について説明する。

まず、ユーザからのアクセスがあると、先に説明した図10と同様の画面がユーザの操作する端末2に表示される。ここで、ユーザが、既にIDを取得している場合、ユーザ名とパスワードを入力することができる。端末2から入力されたIDとパスワードとは通信制御部41を介してアクセス権限レベル制御部44に送られる。ユーザ情報制御部は、IDテーブル管理部45を介してIDデータベース46からIDに対応するパスワードを取得し、端末2を操作するユーザの認

証処理を行う。

【 0 0 4 8 】

なお、IDの取得を望まないユーザからのアクセス、又は、プライオリティレベルが3のユーザからのアクセスに応じては、いずれもパスワードの入力が不要であるため、認証処理は省略されて後続の処理が行われる。

アクセス権限レベル制御部44は認証処理が正常に行われた場合、IDテーブルに登録されたユーザのプライオリティレベルを変数Prに、最終アクセス日をAdに代入する（ステップS201）。この際、アクセス権限レベル制御部44は、登録されたIDに対応するスタートページもIDテーブルから読み出しておく。

【 0 0 4 9 】

この後、アクセス権限レベル制御部44は、Prが4であるか否か判定する（ステップS202）。Prが4である場合（ステップS202：YES）、このプライオリティレベル4と読み出されたスタートページとが情報提供制御部42に通知される。情報提供制御部42は受け取ったスタートページを端末2に表示するための処理を行い、その後、プライオリティレベルに従ってコンテンツデータベース43に保持されているコンテンツの提供を行う（ステップS203）。なお、プライオリティレベル4は、ツアーといういわゆるホームページの構造を見学するためのものであり、ユーザに提供される情報としては最も狭い範囲の情報となる。

【 0 0 5 0 】

Prが4ではない場合（ステップS202：NO）、アクセス権限レベル制御部44は、Prが3であるか否か判定する（ステップS204）。Prが3である場合（ステップS204：YES）、Adに1ヶ月の月日が加算される（ステップS205）。アクセス権限レベル制御部44は図示されないタイマから現在の年月日（現在のアクセス日）を取得し、加算された後のAdと比較する（ステップS206）。

【 0 0 5 1 】

Adが現在のアクセス日より前である場合、すなわち、ユーザのアクセス間隔

が1ヶ月以上ではない場合（ステップS 2 0 6 : YES）、アクセス権限レベル制御部4 4はIDテーブルの最終アクセス日を現在のアクセス日に更新する（ステップS 2 0 7）。この後、プライオリティレベル3と読み出されたスタートページとが情報提供制御部4 2に通知される。情報提供制御部4 2は、受け取ったスタートページを端末2に表示するための処理を行い、その後、プライオリティレベルに従ってコンテンツデータベース4 3に保持されているコンテンツの提供を行う（ステップS 2 0 8）。

## 【 0 0 5 2 】

A dが現在のアクセス日以降である場合、すなわち、ユーザのアクセス間隔が1ヶ月以上である場合（ステップS 2 0 6 : NO）、アクセス権限レベル制御部4 4は、IDテーブルに登録されたユーザの情報を削除すると共に、所定のタイムアウト処理を行う（ステップS 2 0 9）。このタイムアウト処理とは、図1 5に示される画面を端末2に表示させるための処理を含む。同図に示される画面では、IDに対応する有効期限が過ぎており、IDの取得が無効になっていることを通知するための画面である。タイムアウト処理では、この画面に従ったユーザのID再取得、又は、ゲストとしてのホームページの閲覧を支援するための処理である。これにより、一旦IDの登録が消去されたユーザは、再度自己の情報を提供することにより新たなIDを取得することが可能となる。この場合、提供する情報の内容（レベル）を変更することにより、先に割り当てられたプライオリティレベルと異なるプライオリティレベルでのIDを取得することが可能となる。また、IDの取得を望まないユーザは、ゲストとしての情報提供を情報提供システム4に要求することができる。

## 【 0 0 5 3 】

P rが3ではない場合（ステップS 2 0 4 : NO）、アクセス権限レベル制御部4 4は、P rが2であるか否か判定する（図1 4、ステップS 2 1 0）。P rが2である場合（ステップS 2 1 0 : YES）、A dに1年の年月日が加算される（ステップS 2 1 1）。アクセス権限レベル制御部4 4は図示されないタイマから現在の年月日（現在のアクセス年月日）を取得し、加算された後のA dと比較する（ステップS 2 1 2）。



## 【 0 0 5 4 】

A d が現在のアクセス日より前である場合、すなわち、ユーザのアクセス間隔が1年以上ではない場合（ステップ S 2 1 2 : YES）、アクセス権限レベル制御部 4 4 は I D テーブルの最終アクセス日を現在のアクセス日（年月日）に更新する（ステップ S 2 1 3）。この後、プライオリティレベル 2 と読み出されたスタートページとが情報提供制御部 4 2 に通知される。情報提供制御部 4 2 は、受け取ったスタートページを端末 2 に表示するための処理を行い、その後、プライオリティレベルに従ってコンテンツデータベース 4 3 に保持されているコンテンツの提供を行う（ステップ S 2 1 4）。

## 【 0 0 5 5 】

A d が現在のアクセス日以降である場合、すなわち、ユーザのアクセス間隔が1年以上である場合（ステップ S 2 1 2 : NO）、アクセス権限レベル制御部 4 4 は、I D テーブルに登録されたユーザの情報を削除すると共に、所定のタイムアウト処理を行う（ステップ S 2 1 5）。このタイムアウト処理は、前述したステップ S 2 0 9 の処理と同様であるので説明は省略する。

## 【 0 0 5 6 】

P r が 2 ではない場合（ステップ S 2 1 0 : NO）、アクセス権限レベル制御部 4 4 は、P r が 1 であるか否か判定する（ステップ S 2 1 6）。P r が 1 である場合（ステップ S 2 1 6 : YES）、A d に 2 年の年月日が加算される（ステップ S 2 1 7）。アクセス権限レベル制御部 4 4 は図示されないタイマから現在の年月日（現在のアクセス年月日）を取得し、加算された後の A d と比較する（ステップ S 2 1 8）。

## 【 0 0 5 7 】

A d が現在のアクセス日より前である場合、すなわち、ユーザのアクセス間隔が2年以上ではない場合（ステップ S 2 1 8 : YES）、アクセス権限レベル制御部 4 4 は I D テーブルの最終アクセス日を現在のアクセス日（年月日）に更新する（ステップ S 2 1 9）。この後、プライオリティレベル 1 と読み出されたスタートページとが情報提供制御部 4 2 に通知される。情報提供制御部 4 2 は、受け取ったスタートページを端末 2 に表示するための処理を行い、その後、プライオ

リティレベルに従ってコンテンツデータベース 4 3 に保持されているコンテンツの提供を行う（ステップ S 2 2 0）。

## 【 0 0 5 8 】

A d が現在のアクセス日以降である場合、すなわち、ユーザのアクセス間隔が 2 年以上である場合（ステップ S 2 1 8 : N O）、アクセス権限レベル制御部 4 4 は、I D テーブルに登録されたユーザの情報を削除すると共に、所定のタイムアウト処理を行う（ステップ S 2 2 1）。このタイムアウト処理は、前述したステップ S 2 0 9 の処理と同様であるので説明は省略する。

## 【 0 0 5 9 】

P r が 1 ではない場合（ステップ S 2 1 6 : N O）、アクセス権限レベル制御部 4 4 は、アクセスしてきたユーザが、プライオリティレベル 0 の管理者であると判断し、I D テーブルの管理者に対応するアクセス日を現在のアクセス日に更新する（ステップ S 2 2 2）。この後、プライオリティレベル 0 と読み出されたスタートページとが情報提供制御部 4 2 に通知される。情報提供制御部 4 2 は、受け取ったスタートページを端末 2 に表示するための処理を行い、その後、プライオリティレベルに従ってコンテンツデータベース 4 3 に保持されているコンテンツの提供を行う（ステップ S 2 2 3）。

## 【 0 0 6 0 】

以上の処理により、プライオリティレベルに応じた範囲内での情報提供が行われる。特にこの第 2 実施形態では、I D 登録する際に、情報提供システム 4 に提供されるユーザの個人情報の内容に従って、提供可能な情報の範囲を定めるプライオリティレベルが設定される。従って、情報提供システム 4 を運営・管理する者は、登録されたユーザがどの程度提供する情報に関心を持っているかを判断することができる。

さらに、登録後の関心がどのように変化しているかも検出することができ、ユーザから得られた個人情報や提供する情報にこれを利用することもできる。すなわち、提供される情報に対するユーザの関心が低下した場合、情報提供システム 4 にアクセスする間隔が長くなる。このため、多くのユーザのアクセス間隔が長くなった場合には、コンテンツデータとしてユーザに提供している情報を見直す

こともできる。

【 0 0 6 1 】

また、予めプライオリティレベル毎に所定の時間間隔を設定し、この設定を越えた場合にユーザの関心が低下したと判断し、IDテーブルの登録が削除される。従って、IDテーブルに提供情報に対する関心が所定の度合い以上低下した場合には登録が削除されるため、必要なユーザに対する情報のみを管理することができる。ただし、登録が削除された後でも、ユーザは再登録（IDの再取得）が可能であるため、一旦関心が低下した後でもユーザは情報の提供を得ることができる。

なお、この第2実施形態では、IDテーブルからの削除処理をユーザからのアクセスをトリガとして行っているがこれに限らず、たとえば、定期的に時間経過を通知するタイマを用いてアクセスの有無に関係無く定期的に行うようにしてもよい。

【 0 0 6 2 】

以上第1及び第2実施形態を用いて説明したように本発明によれば、提供する処理環境や情報に対するユーザの関心度合及び／又はその変化が定量化され、これが用いられることにより、ユーザに対する処理環境や情報の提供範囲を定める情報を制御することができる。従って、優良なユーザにはそれに見合った処理環境や情報を提供することが可能となる。

【 0 0 6 3 】

なお、第1実施形態では、アクセス権限レベルに「シェル」、関心度合い及び／又はその変化を検出するための情報に「パスワード変更回数」、ユーザへの提供対象に「処理環境」を用い、第2実施形態ではこれらそれぞれに「プライオリティレベル」、「最終アクセス日からの経過日数」、「情報」を用いているがこれに限らない。これらの組合せを変更したり、共用することも可能である。

また、関心度合い及び／又はその変化の定量化には、ログイン回数、登録後の継続期間（例えば、ユーザが登録により会員となる場合にはその会員継続期間）、又は他のユーザを紹介した場合などのユーザ行為をポイントに換算してそのユーザに付与するポイント付与を適用することもできる。この際、ユーザの行為内

容に応じたポイント数割当を設定しておくことにより、ユーザの関心度合い及び／又はその変化を効果的に定量化することができる。付与されたポイントは累積加算したり、所定のポイント数から減算することに用いてもよい。従って、前述した実施形態におけるIDテーブルでは、これらのポイント加算又は減算結果を記録するための欄を新たに設ける必要がある。

#### 【0064】

この他、定量化されたユーザの関心度合い及び／又はその変化に従って、ユーザに対する処理環境や情報の提供範囲を定める情報、すなわちアクセス権限レベルを制御するとともに、他の要因に従ってアクセス権限レベルを制御してもよい。

例えば、ユーザが登録後に会員として扱われる場合、会員となった直後の一定期間を会員の初心者向けの処理環境や情報が提供されるようにアクセス権限レベルを制御したり、登録後から特定期間が経過する前後に特別な処理環境や情報を提供するようにアクセス権限レベルを制御してもよい。特定期間経過前後とは、提供対象物がホームページに掲載される情報である場合、会員登録後1年間経過したときに加入1年目のプレミアムページの閲覧を会員が可能となるようにすることもできる。登録の際にユーザから誕生日などの特定の日時に関する情報が提供された場合には、提供された日時の当日またはその前後などに特別な処理環境や情報が提供されるようにアクセス権限レベルを変更してもよい。

#### 【0065】

##### 【発明の効果】

本発明により各ユーザに対して適切な情報範囲内の情報や処理環境を提供を行うための技術が提供される。特に提供可能な情報や処理環境の範囲を定める複数レベルのアクセス権限をユーザ毎に適宜制御するための装置及び方法が提供される。

##### 【図面の簡単な説明】

##### 【図1】

本発明を適用した処理環境提供システムの実施形態（第1実施形態）の構成を示すブロック図。

【図 2】

処理環境提供システムの I D データベースに保持されている I D テーブルの一例。

【図 3】

処理環境提供システムにおいて、ユーザからログインを受け付けてからの処理を説明するための手順説明図。

【図 4】

ログイン時にユーザの操作する端末に表示される画面例。

【図 5】

パスワード変更が要求されたユーザの操作する端末に表示される画面例。

【図 6】

パスワード変更要求にユーザが応じたことにより更新された I D テーブルの一例。

【図 7】

パスワード変更要求にユーザが応じなかった場合に更新された I D テーブルの一例。

【図 8】

本発明を適用した情報提供システムの実施形態（第 2 実施形態）の構成を示すブロック図。

【図 9】

情報提供システムの I D データベースに保持されている I D テーブルの一例。

【図 1 0】

ユーザからの情報提供要求に応じてユーザの操作する端末に表示される画面例。

【図 1 1】

図 1 0 の画面例に従って、ユーザが I D の取得のみを望んだ場合に更新された I D テーブルの一例。

【図 1 2】

図 1 0 の画面例に従って、ユーザが自己の名前と電話番号を通知することによ

り I D の取得の望んだ場合に更新された I D テーブルの一例。

【図 1 3】

既に I D を取得したユーザ、又は I D の取得の望まないユーザのアクセスに応じた情報提供システム 4 の処理を説明するための手順説明図。

【図 1 4】

既に I D を取得したユーザ、又は I D の取得の望まないユーザのアクセスに応じた情報提供システム 4 の処理を説明するための手順説明図。

【図 1 5】

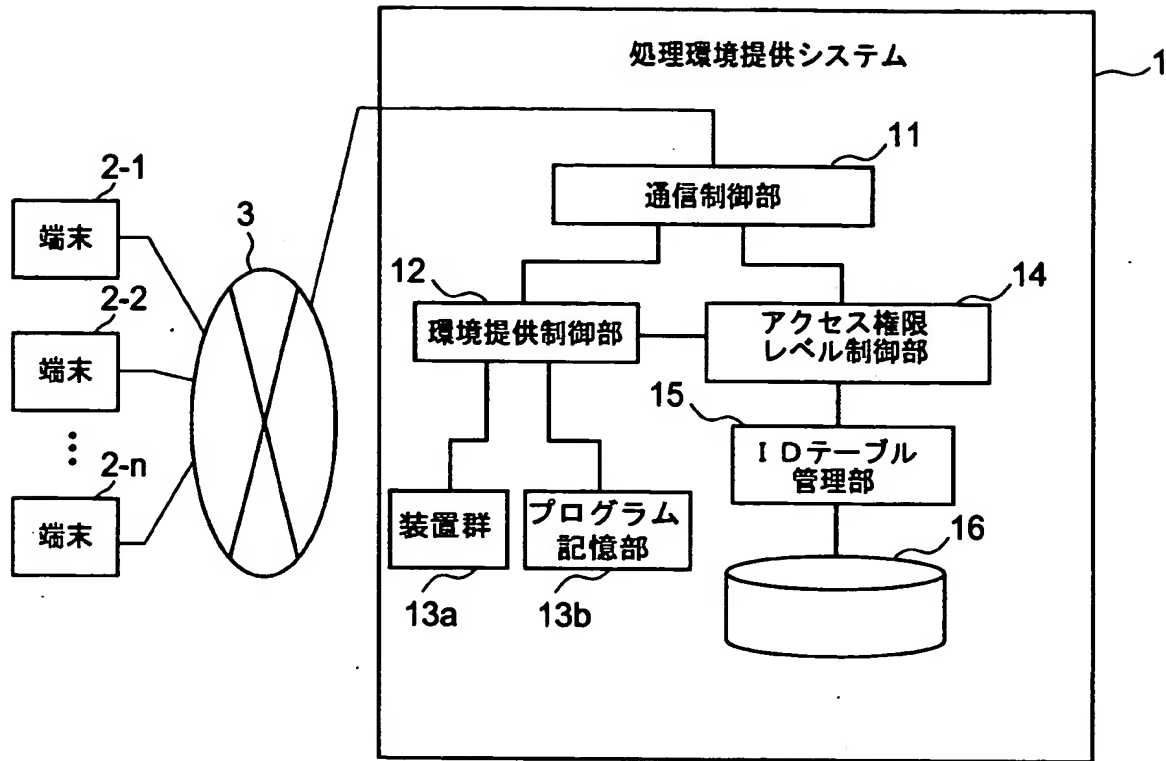
図 1 4 及び図 1 5 の手順において、ユーザのアクセス間隔がユーザのプライオリティレベルに応じた間隔を越えた場合に、ユーザの操作する端末に表示される画面例。

【符号の説明】

- 1 処理環境提供システム
- 2 - 1 ~ 2 - n 端末
- 3 ネットワーク
- 4 情報提供システム
- 1 1 通信制御部
- 1 2 環境提供制御部
- 1 3 a 装置群
- 1 3 b プログラム記憶部
- 1 4 アクセス権限レベル制御部
- 1 5 I D テーブル管理部
- 1 6 I D データベース
- 4 1 通信制御部
- 4 2 情報提供制御部
- 4 3 コンテンツデータベース
- 4 4 アクセス権限レベル制御部
- 4 5 I D テーブル管理部
- 4 6 I D データベース

【書類名】 図面

【図 1】

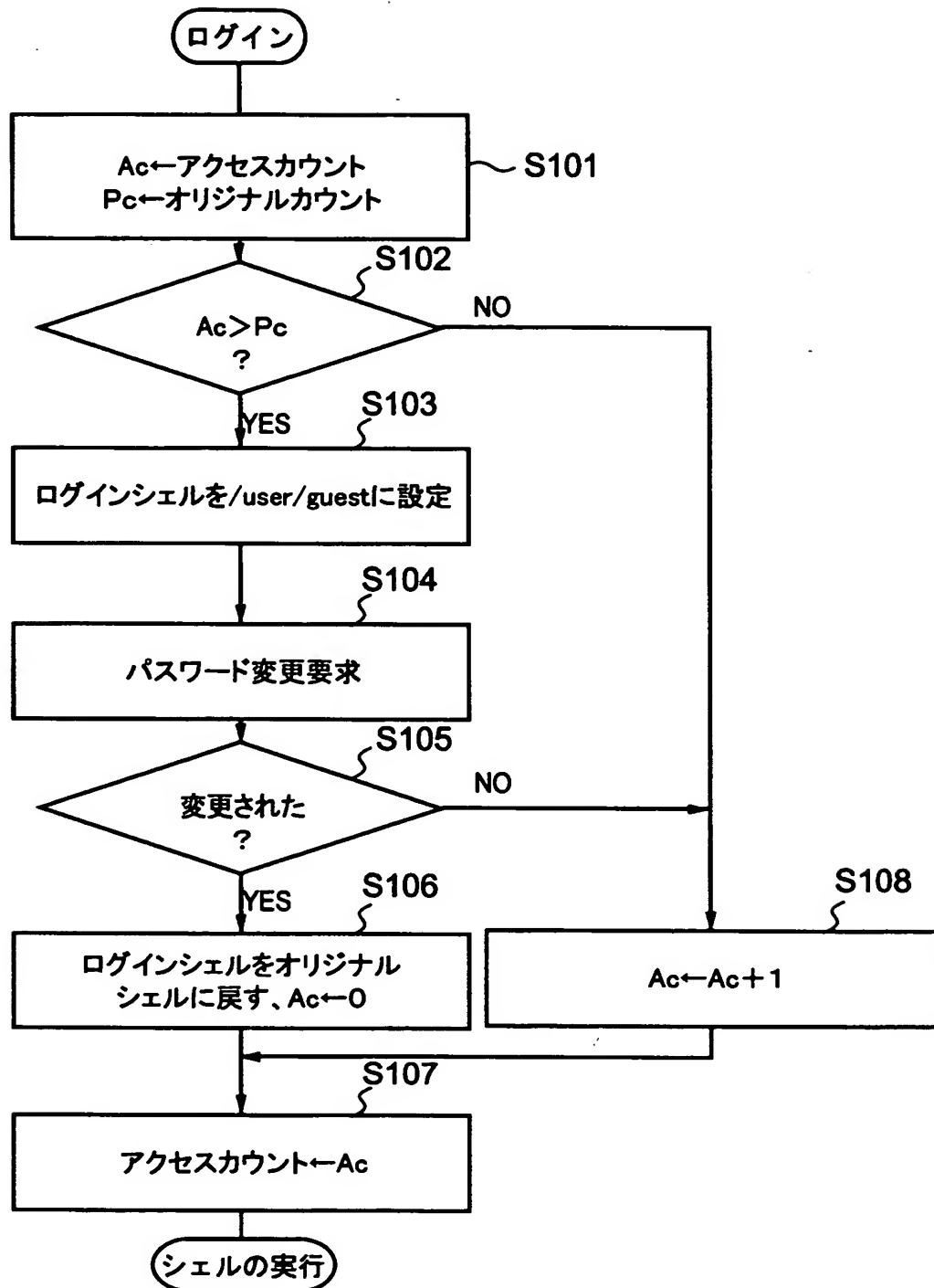


【図 2】

ID	パスワード	アクセス カウント	プライオリティ カウント	ログイン シェル	オリジナル シェル
管理者	*****	12	29	/	/
ユーザ1	*****	9	99	/user/user1	/user/user1
ユーザ2	ABCDE	100	99	/user/user2	/user/user2
⋮	⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	999999999	/user/guest	/user/gest



【図 3】



【図 4】

please log in:

user\_id

password

Guest login is available.  
Please type "guest" in user\_id without password  
ゲストログインが可能です。  
その場合ユーザidに"guest"と入力してください。  
パスワードの入力は不要です。

【図 5】

Attention お知らせ

Your access count over 100 times. Please change password for security. If you will not change it, you will lose your premium access.  
あなたのアクセス回数が100回を越えました安全のためパスワードの変更を行ってください。変更が行われない場合は、アクセスに制限が加わる場合があります。

New\_Password

type again

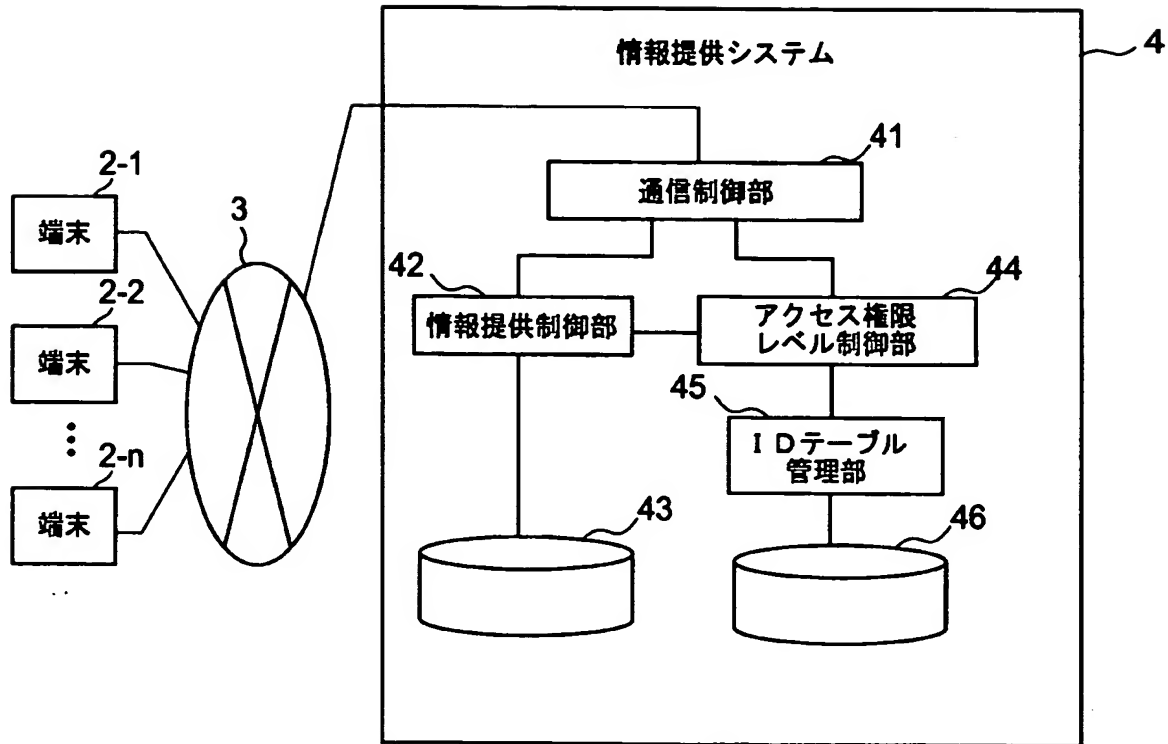
【図 6】

ID	パスワード	アクセス カウント	プライオリティ カウント	ログイン シェル	オリジナル シェル
管理者	*****	12	29	/	/
ユーザ1	*****	9	99	/user/user1	/user/user1
ユーザ2	FGHIJ	0	99	/user/user2	/user/user2
⋮	⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	999999999	/user/guest	/user/guest

【図 7】

ID	パスワード	アクセス カウント	プライオリティ カウント	ログイン シェル	オリジナル シェル
管理者	*****	12	29	/	/
ユーザ1	*****	9	99	/user/user1	/user/user1
ユーザ2	ABCDE	101	99	/user/guest	/user/user2
⋮	⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	999999999	/user/guest	/user/guest

【図 8】



【図 9】

ID	パスワード	最終 アクセス日	プライオリティ レベル	スタートページ
管理者	*****	2000/08/08	0	/admin. html
ユーザ001	*****	2000/08/15	1	/level1/index. html
ユーザ002	*****	2000/09/10	2	/level1/level2/index. html
⋮	⋮	⋮	⋮	⋮
ユーザ302	なし	2999/12/31	99	/level1/level2/level3/index. html
⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	4	/level1/level2/level3/tour. html

【図 10】

[illegible]

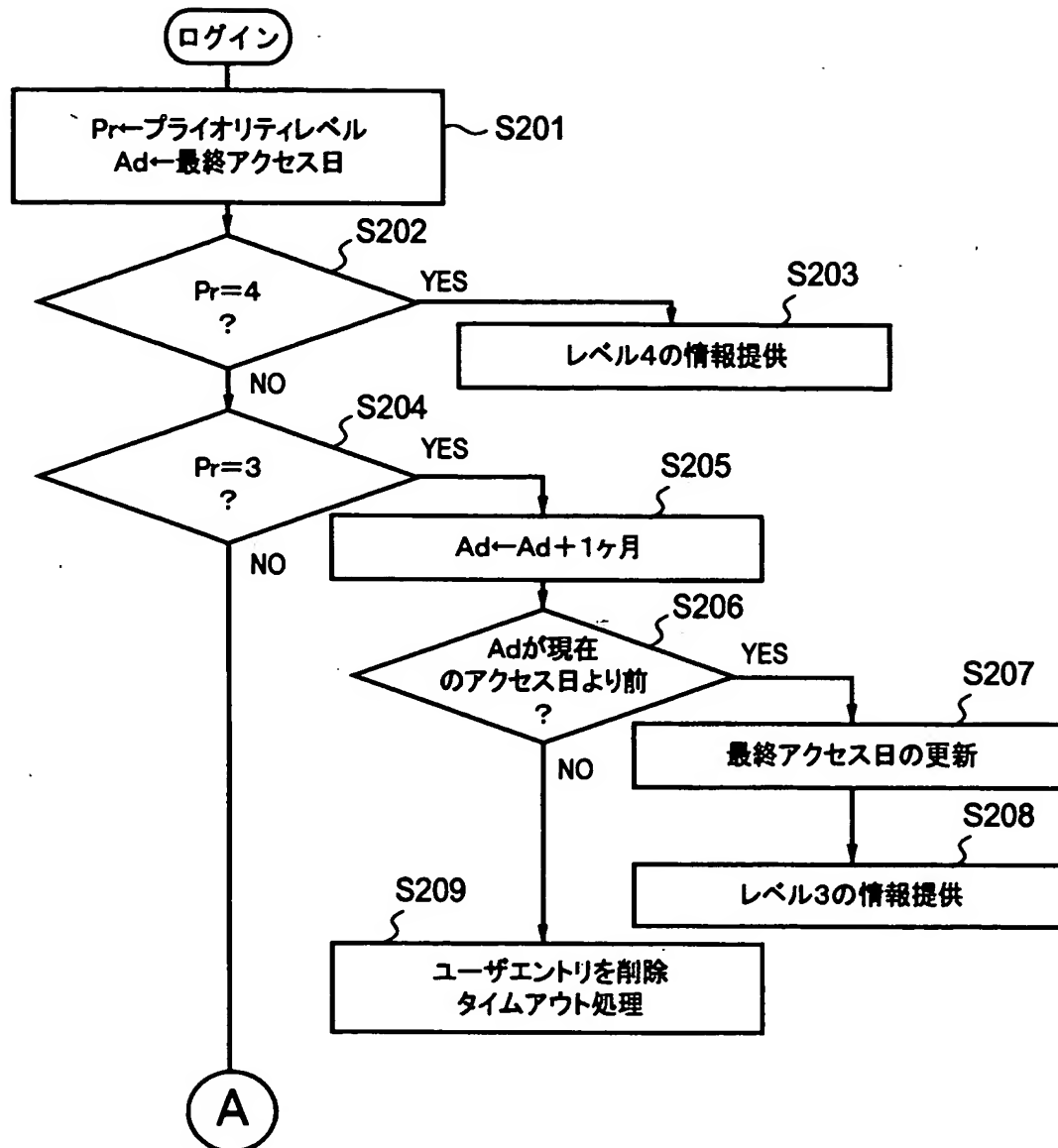
【図 1 1】

I D	パスワード	最終 アクセス日	プライオリティ レベル	スタートページ
管理者	*****	2000/08/08	0	/admin. html
ユーザ001	*****	2000/08/15	1	/level1/index. html
ユーザ002	*****	2000/09/10	2	/level1/level2/index. html
⋮	⋮	⋮	⋮	⋮
ユーザ302	なし	2000/10/01	3	/level1/level2/level3/index. html
⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	4	/level1/level2/level3/tour. html

【図 1 2】

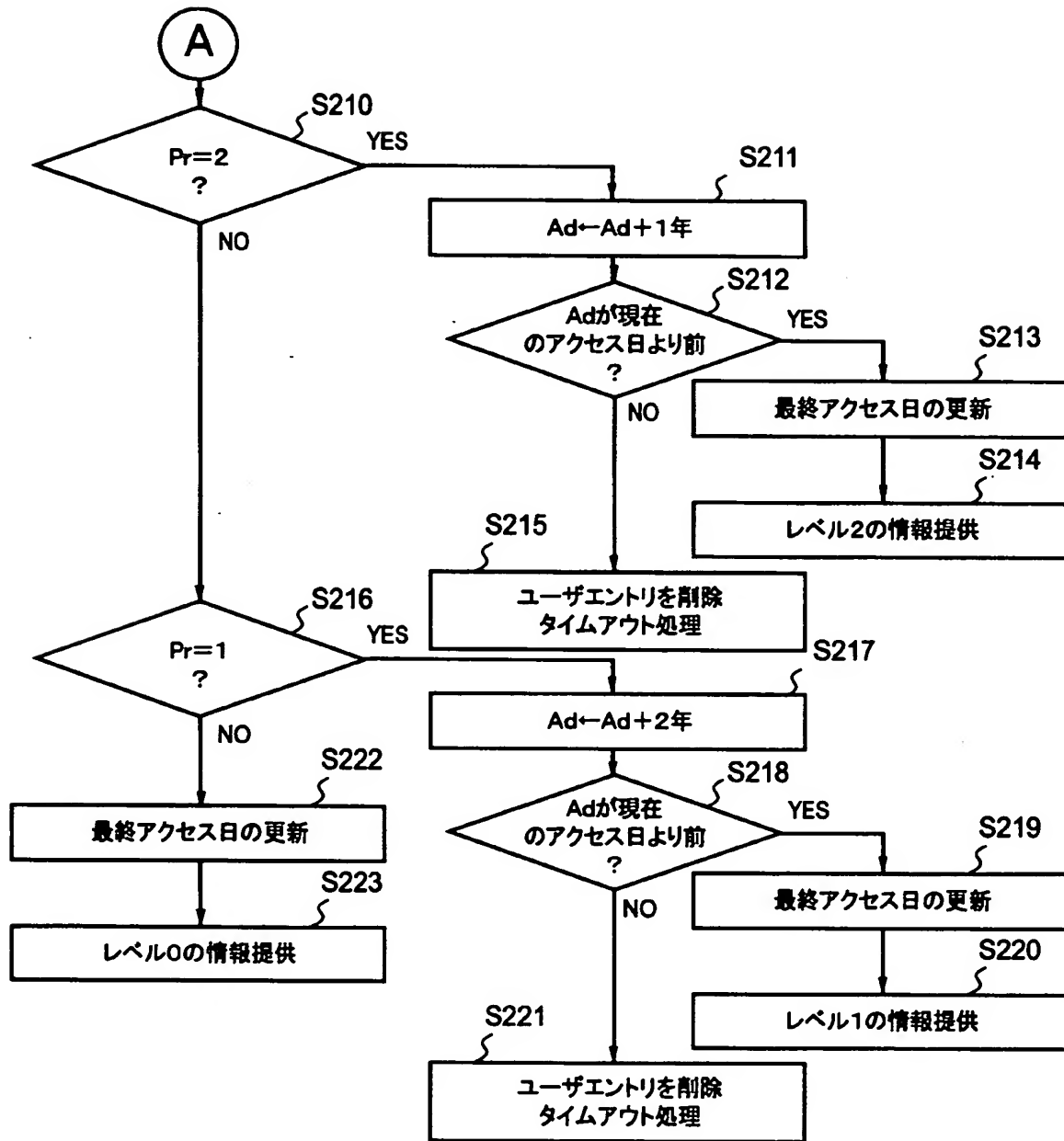
I D	パスワード	最終 アクセス日	プライオリティ レベル	スタートページ
管理者	*****	2000/08/08	0	/admin. html
ユーザ001	*****	2000/08/15	1	/level1/index. html
ユーザ002	*****	2000/09/10	2	/level1/level2/index. html
⋮	⋮	⋮	⋮	⋮
ユーザ302	KLMNO	2000/10/01	2	/level1/level2/index. html
⋮	⋮	⋮	⋮	⋮
ゲスト	なし	0	4	/level1/level2/level3/tour. html

【図 1 3】





【図14】



【図15】

<a href="#">ホーム</a> <a href="#">お気に入り</a> <a href="#">履歴</a> <a href="#">印刷</a>	
<a href="#">ファイル名</a> <a href="#">編集</a> <a href="#">お気に入り</a> <a href="#">ブックマーク</a> <a href="#">ヘルプ</a>	
<a href="#">アドレス</a> <a href="#">http://www.***.com/time-out.asp</a>	

勝手ではありますが、お客様のIDは有効期限が過ぎている為に抹消されています。再度下記フォームにて登録を行って下さい。

**IDは取得しない** IDの取得がない場合、アクセスできるページはツアーのみです。

---

**IDのみの取得** IDは自動的に発行されます。パスワードはありません。  
 取得されたIDの有効期限は1ヶ月です。期間内に再アクセスがない場合はIDは抹消されます。また、個人情報を登録した場合はパスワードを定めるページと、有効期限が過ぎます。

---

**電話番号と名前を登録** 電話番号はご自宅の電話を登録下さい。  
 IDとパスワードは自動的に発行されます。  
 取得されたIDの有効期限は1年間です。期間内に再アクセスがない場合はIDは抹消されます。

---

**詳細な個人情報を登録**

電話  -  -  (半角数字)  
 住所  (全角漢字)  
 氏名  (全角漢字)  (半角カナ)  
 性別 男○ 女○ 年齢 ~15歳○ 16歳~19歳○ 20歳~29歳○ 30歳~45歳○ 45歳~○

【書類名】 要約書

【要約】

【課題】 提供可能な情報や処理環境の範囲を定める複数レベルのアクセス権限をユーザ毎に適宜制御する。

【解決手段】 処理環境提供システム 1 のアクセス権限レベル制御部 1 4 は端末 2 からのアクセスに応じ、ID データベース 1 6 に記憶されているパスワード変更後のアクセス数と予め割り当てられているプライオリティカウントとを比較する。変更後のアクセス数がプライオリティカウントを越えた場合に端末 2 を操作するユーザにパスワードの変更処理を促す。パスワードが変更された場合には先に割り当てられているアクセス権限のレベルを、そうでない場合には提供される処理環境が制限されたアクセス権限のレベルが環境提供制御部 1 2 に通知される。環境提供制御部 1 2 は通知されたレベルに従って端末 2 に処理環境を提供する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002369]

1. 変更年月日	1990年 8月20日
[変更理由]	新規登録
住 所	東京都新宿区西新宿2丁目4番1号
氏 名	セイコーエプソン株式会社